Military Cryptographic Systems

Information Assurance Block

Objective

Students will learn about the most common military cryptographic systems such as the KG-84, KIV-7, KIV-19, STE and KG-75 to include data rates, price, and practical applications. On conclusion of this block, the students will be able to choose which particular cryptographic device to use to encrypt a link given the data rate, terminal equipment and transmission medium.

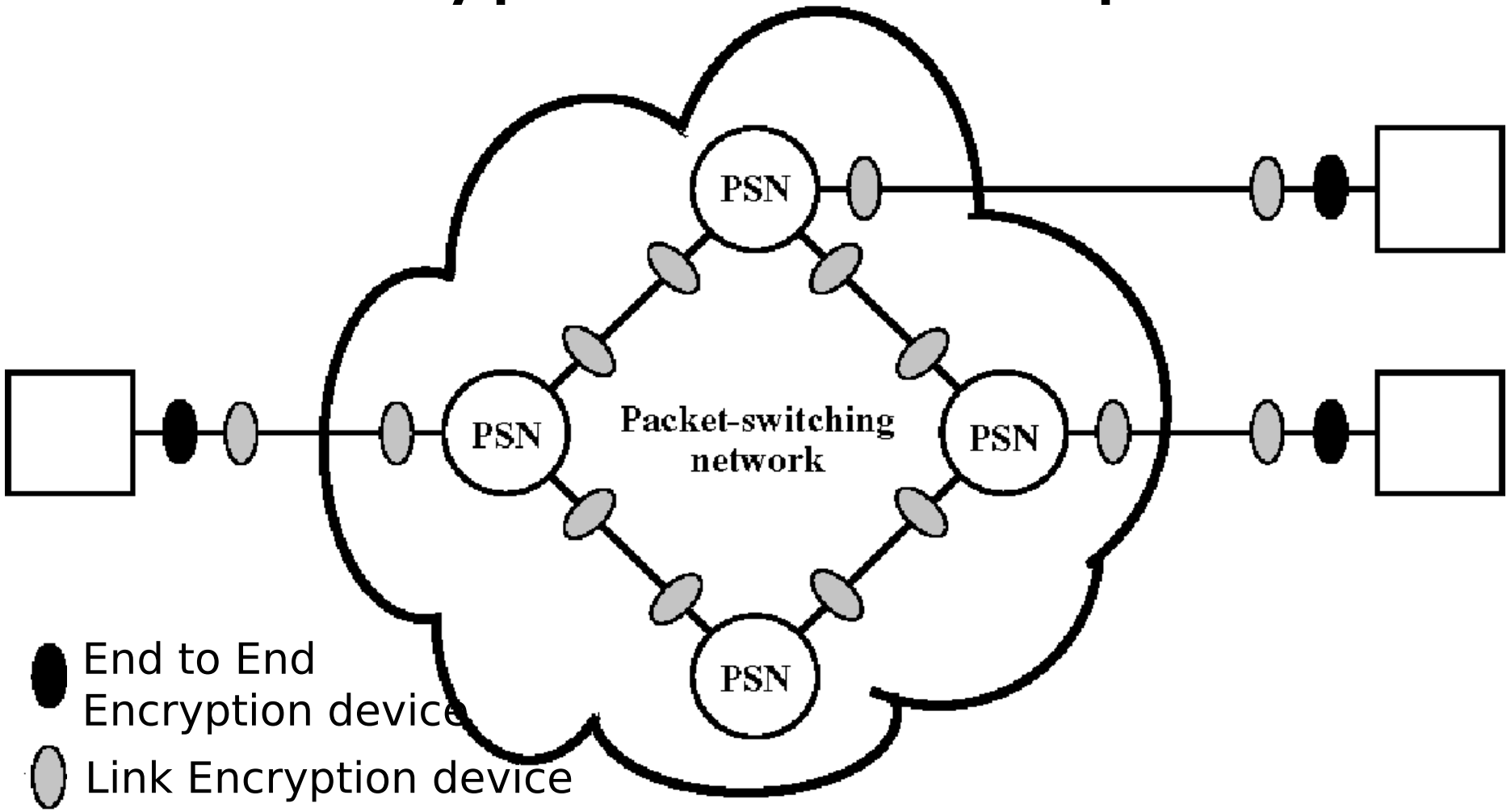
Outline

- Encryption Techniques
- Black/Red Signal
- Cryptographic Standards
- NSA Cryptographic Types
- Layer 1 Military Cryptographic Equipment
- Layer 2 Military Cryptographic Equipment
- Layer 3 Military Cryptographic Equipment
- Telephony Cryptographic Equipment
- Fill Devices
- Key Generators
- Summary

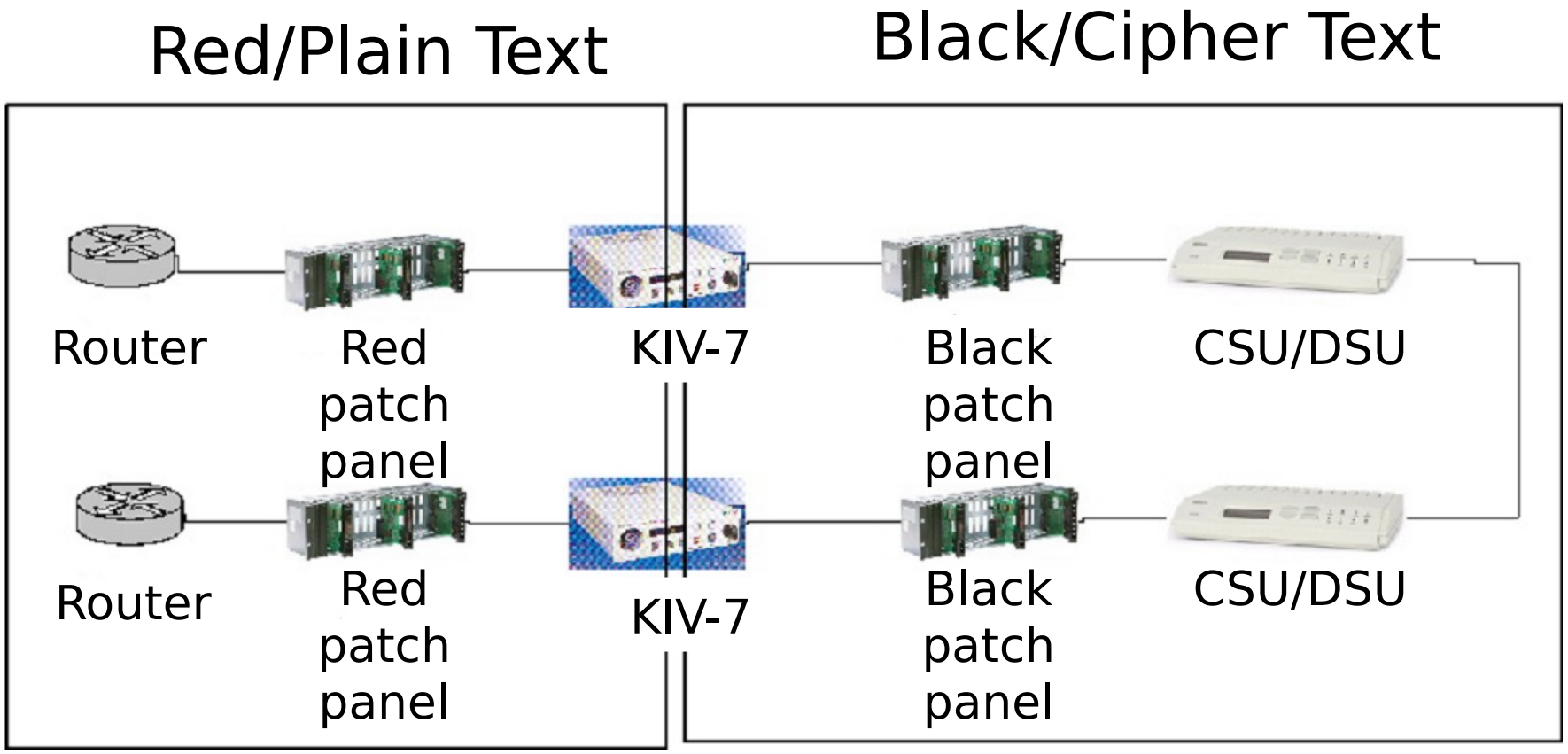
Encryption Techniques

- End-to-end
  - PKI
  - STU-III/STE/Red Switch
- Link
  - Most military secure data networks
  - Bases overseas include additional layer of encryption -- called TRANSEC (Transport Security) usually at DS3 or OC3 level

Encryption Techniques



Black/Red Signals



Cryptographic Standards

- **NSA**
  - Secret and above
  - Type 1 encryption required
  - Algorithms are classified
- **National Institute of Standards and Technology (NIST)**
  - Set standards for SBU traffic
  - de facto standards organization for commercial businesses

Cryptographic Standards

- **American National Standards Institute (ANSI)**
  - Important cryptographic standards organization for the U.S.
  - ANSI X9 series closely mirrors NIST's Federal Information Processing Standard (FIPS)
- **International Organization of Standards (ISO)**
  - Overall ISO is not that involved with security standards with the exception of X.509 and Common Criteria

Approved Cryptosystems

The only cryptosystems approved for US Army use are those systems which are:

- Produced by NSA
- Commercial “Off the Shelf” Systems approved by NSA for local purchase
- Electronically generated and distributed using NSA approved key generating equipment and procedures IAW NAG 16

TB 380-41 Section 3.3.

NSA Cryptographic Types

- Type 1
  - U.S. government and military for Classified Information
  - Only approved commercial users are defense contractors working on U.S. classified projects
  - KIV-21, NES, Sectera, KOV-14, CONDOR, STU-III
- Type 2
  - US government for SBU information
  - Requires U.S. government agency sponsorship
  - KOV-14, MYK-3B, STU-III

NSA Cryptographic Types

- Type 3
  - Can only be exported to U.S. corporations abroad, and must be under the control of U.S. citizen.
- Type 4
  - Exportable to any country and organization, except those prohibited by the U.S. government

Cryptographic Equipment

Layer 1 (Physical)

- KG-84
- KIV-7
- KG-194
- KIV-19
- KG-189

Layer 2 (Data link)

- KG-75
- KG-175 (2 and 3)
- KIV-21

Layer 3 (Network)

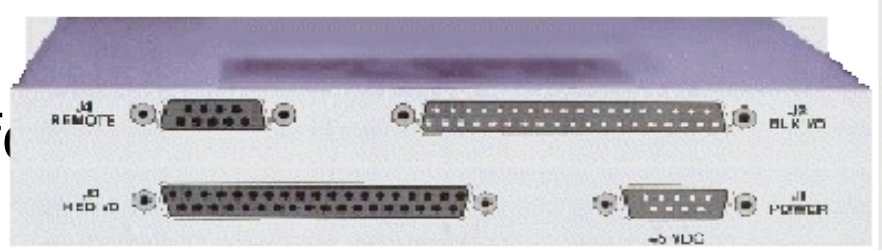
- KG-175 (2 and 3)
- Network Encryption System (NES)

KG-84

- KG-84A -- 256 kbps
- KG-84C -- 64 kbps
- Uses military standard canon plug
- Can operate from 50 to 9600 Mbps async
- Can process up to 32 Kbps usir internal clock
- Includes built-in wireline mode
- No longer produced

KIV-7

- Four models
  - KIV-7 512 Kbps
  - KIV-7HS 1.544 Mbps
  - KIV-7HSA/B 2.048 Mbps
- Interoperable with KG-84
- Serial Data Interfaces
  - EIA-530, EIA-449, EIA-232
- Removable CIK
- No internal strappings
- Optional Wireline Module fo
  Tactical



KIV-7 Prices

- KIV-7 – No longer produced
- KIV-7HS -- $3,555
- KIV-7HSA -- $3,900
- KIV-7 Rack Assemblies
  - Dual Bay Model 3014-1 - $635
  - Dual Bay Model 3014-2 - $690
  - Four Bay Model 3016-1 - $890
  - Four Bay Model 3018-1 - $985
  - Eight Bay Model 3018-1 - $990
  - Eight Bay Model 3018-2 - $1,010

KG-194

- KG-94/94A/194/194A
- Operates from 9.6 kbps to 13 Mbps
- Use traditional or firefly key
- Two versions -- tactical and fixed plant

KIV-19

- Operates from 9.6 kbps to 13 Mbps
- Use traditional or firefly key
- Compatible with KG-194
- Newest version KIV-19A (no internal strapping)

KIV-19 Prices

- KIV-19 - $3,692
- KIV-19 Rack Mounts
  - Single Model 5020-1 - $1,635
  - Dual Tray Rack Mount Model 5020-2 - $2,665
- KG-194 Rack Mounts
  - Pulse Engineering 3023-14 - $4,821
  - Pulse Engineering 3023-16 - $4,821
  - HNF-81 Crypto Frame - $3,025

KG-95

- DS3 encryptor
- No longer being produced
- Bulk Encryption
- Three models
  - KG-95-1 capable of operating from 10-50 Mbs
  - KG-95-2 operates only at DS-3 rate
  - KG-95R two KG-95-2s together

KG-189

- SONET Encryptor
- Operates at OC-3, OC-12 and OC-48
- Type I encryption
- F/O Interface
- Firefly key
- $65,000

KG-75 (FASTLANE)

- ATM encryptor
- KG-75 supports up to OC-12
- KG-75A supports up to OC-192
- Interoperable with KG-175 (TACLANE)
- Supports up to 4094 simultaneous, cryptographically isolated ATM channels
- Supports DS1, DS3, OC3C and OC12C
- Supports PNNI 1.0, UNI 4.0 and SNMP
- Firefly and traditional key
- Must use CYZ-10/DTD

KG-75 Pricelist

- KG-75 w/DS3 Interface - $26,985
- KG-75 w/OC3 MM Interface - $26,924
- KG-75 w/OC3 SM Interface- $27,921
- Annual H/W & S/W Maintenance - $5,975

KG-175 (TACLANE)

- ATM Encryption -- 45 Mbps
  - DS3 BNC connector
  - ATM (AAL 1, ¾, 5)
  - PVC and SVC
  - 253 cryptographically isolated channels
- IP Encryption -- 7.2 Mbps
  - RJ-45 and AUI connector
- UNI 4.0 and SNMPv1
- Firefly and traditional key
- Must use CYZ-10/DTD
- Cost $8,124
- E-100 version provides IP encryptio

KIV-21

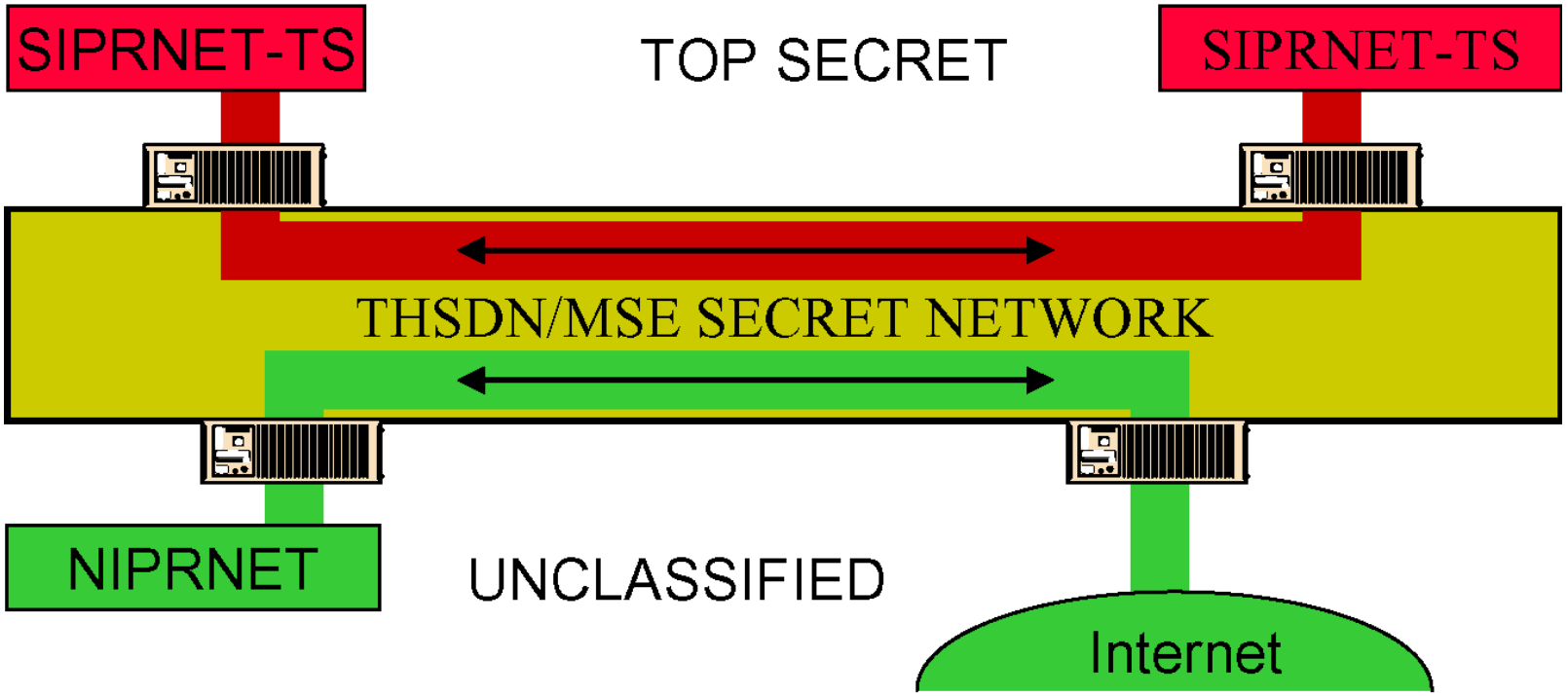
- Converts black EIA-422, DB37 HDLC into red IEEE 802.11 ethernet
- Can be used in lieu of a KIV-7/KG-84/KG-194 and CSU/DSU for site with a single workstation
- Throughput is 8 Kbps to 3 Mbps
- Frame relay
- $13,425

Network Encryption System (NE

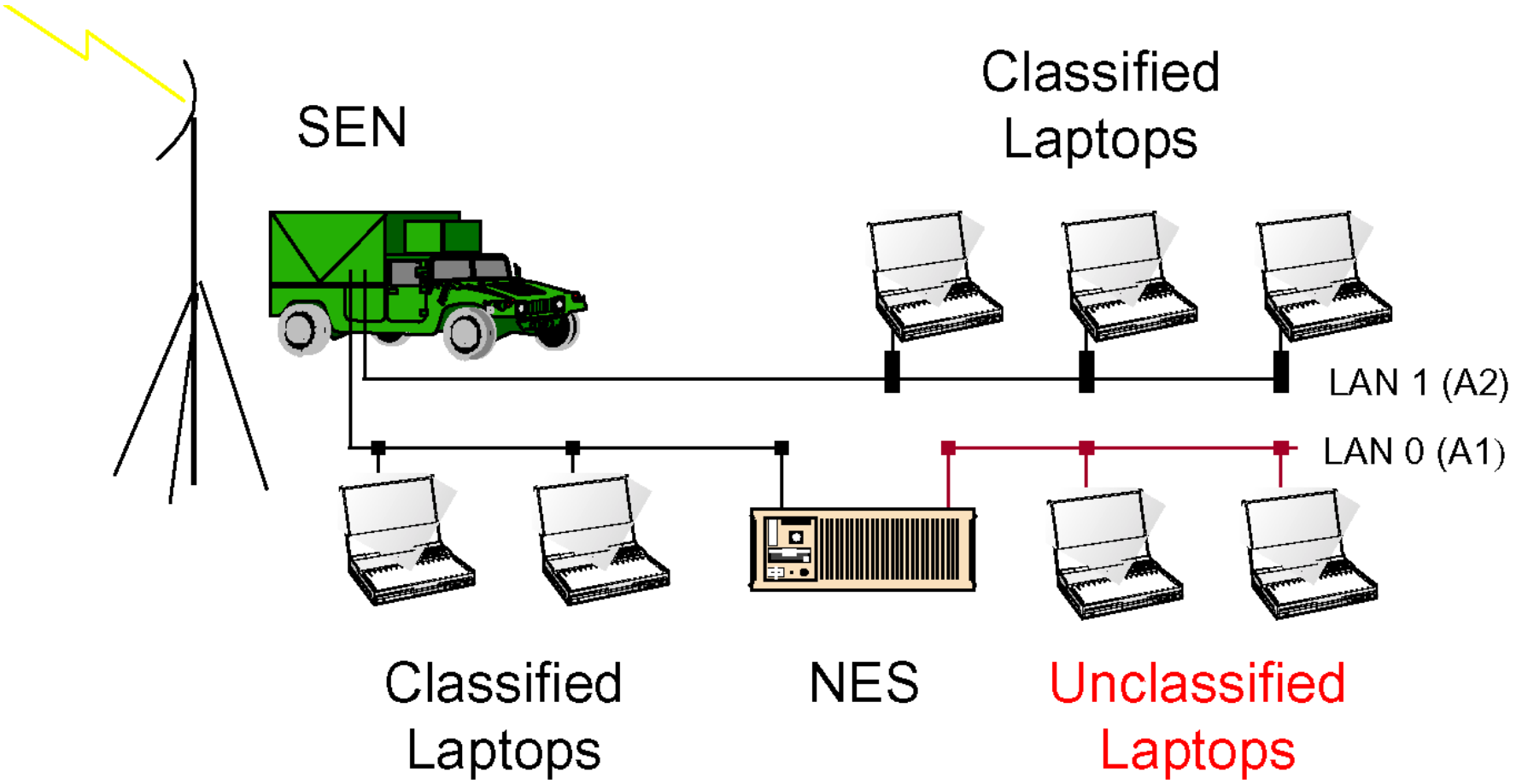
- IP Encryption
- NES 4001A has throughput of 4.3 Mbps
- NES 4001 supports up to 3.4 Mbps
- Older legacy IPA and IP models only support up to 1.3 Mbps
- Required black and red IP addresses
- Uses FIREFLY electronic key distribution

Network Encryption System

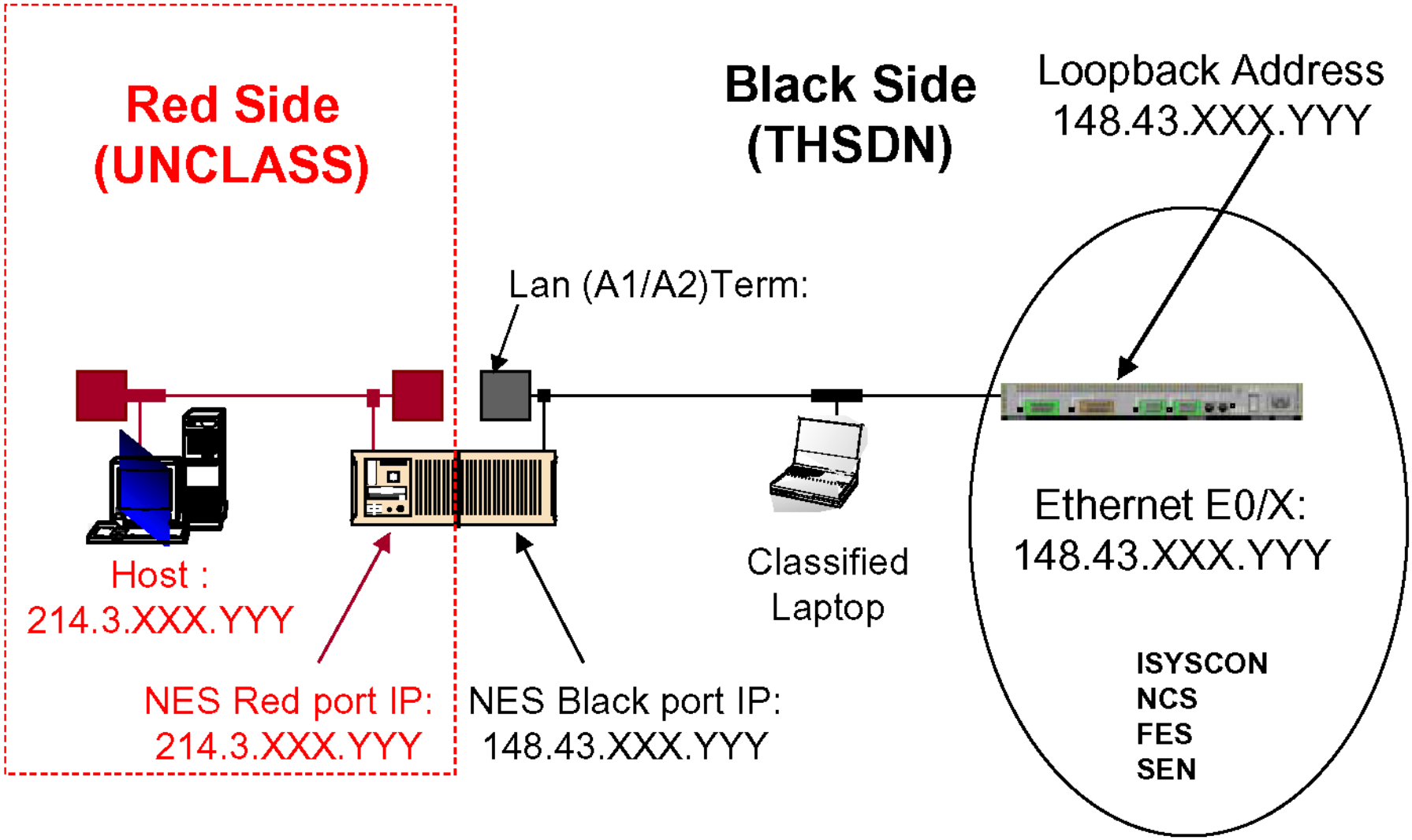
Virtual Private Network (VPN) which permits traffic from one network to *tunnel* through another network of a dissimilar security classification



SEN with NES


SEN
Classified
Laptops
LAN 1 (A2)
LAN 0 (A1)
Classified
Laptops
NES
Unclassified
Laptops

NES Black/Red Separation



Cryptographic Equipment

Telephony

- STU-III
- STE
- Omni
- Secure Cell Phones
- KY-68
- FNBDT

STU-III

- Operate at 2.4 or 4.8 kbps code-excited line prediction (CELP)
- Data transmitted at 2.4, 4.8 and 9.6 kbps
- Supports the ITU-T standards
  - V.26bit
  - V.26ter
  - V.32

STE

- Replacement for STU-III and KY-68
- ISDN (2B+D) and POTS compatible
- Uses four wire S/T interface (NT1 may be required)
- Key is Fortezza Plus (KOV-14)
- Allies use
  - KOV-15 – NATO
  - SOV-16 -- Others
- Price is $3250 – card is $255
- Tactical is $3750
- Interoperable with
  - STU-III (STE in STU mode, not FNBDT)
  - DNVT (Tactical only)
  - ISDN: NI-1, NI-2, 5ESS, DMS-100, DEFINITY
  - Euro ISDN (ETSI-3)

STE Interfaces

- Network Interface
  - ISDN S/T BRI – 1B+D or 2B+D – RJ-45
  - PSTN – RJ-11
  - TRI-TAC/MSE wire line modem – 4 wire (tactical only)
  - EIA-232/530A (tactical only)
- Host Interface
  - EIA-232/530A

Omni

- Secure Terminal provides Type-1 security for voice and data
- Analog and Digital network
- FNBDT compliant
- Compatible with POTs and STU-III
- L3 Communications

Secure Cell Phones (1 of 2)

Motorola Cipher-Tac 2000

- STU-III and STE compatible
- Type 1 analog cellular security
- sleeve slides between battery and phone to operate in secure mode
- no longer in production

Qualcomm Qsec 800

- Secure voice and data (CMI
- Type 1 analog cellular secur
- requires no add-on module

Secure Cell Phones (2 of 2)

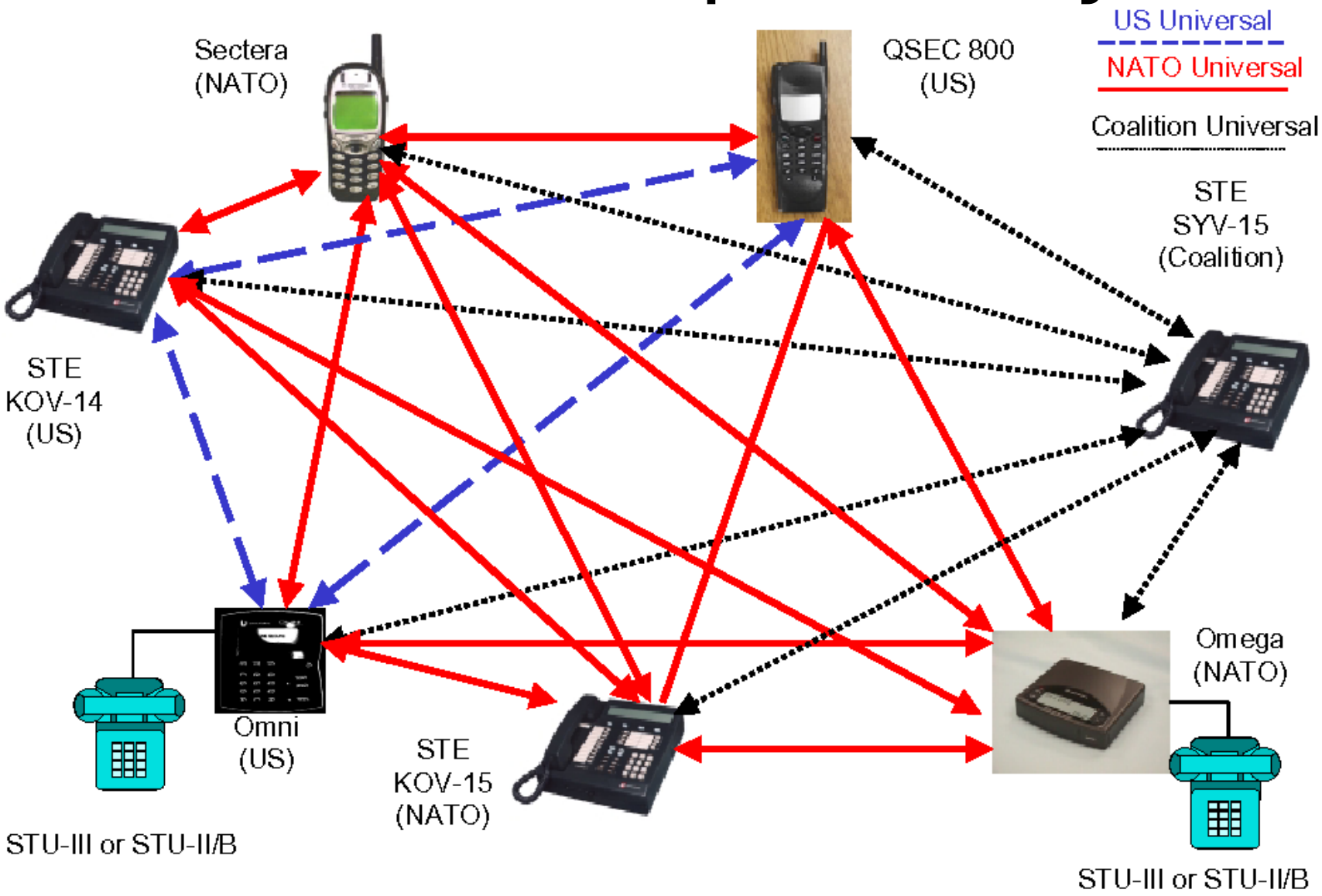
General Dynamics

- Tri-band (GSM 900/1800/1900)
- Advanced Encryption Standard (AES)
- Clip-in security module
- Type 1 security

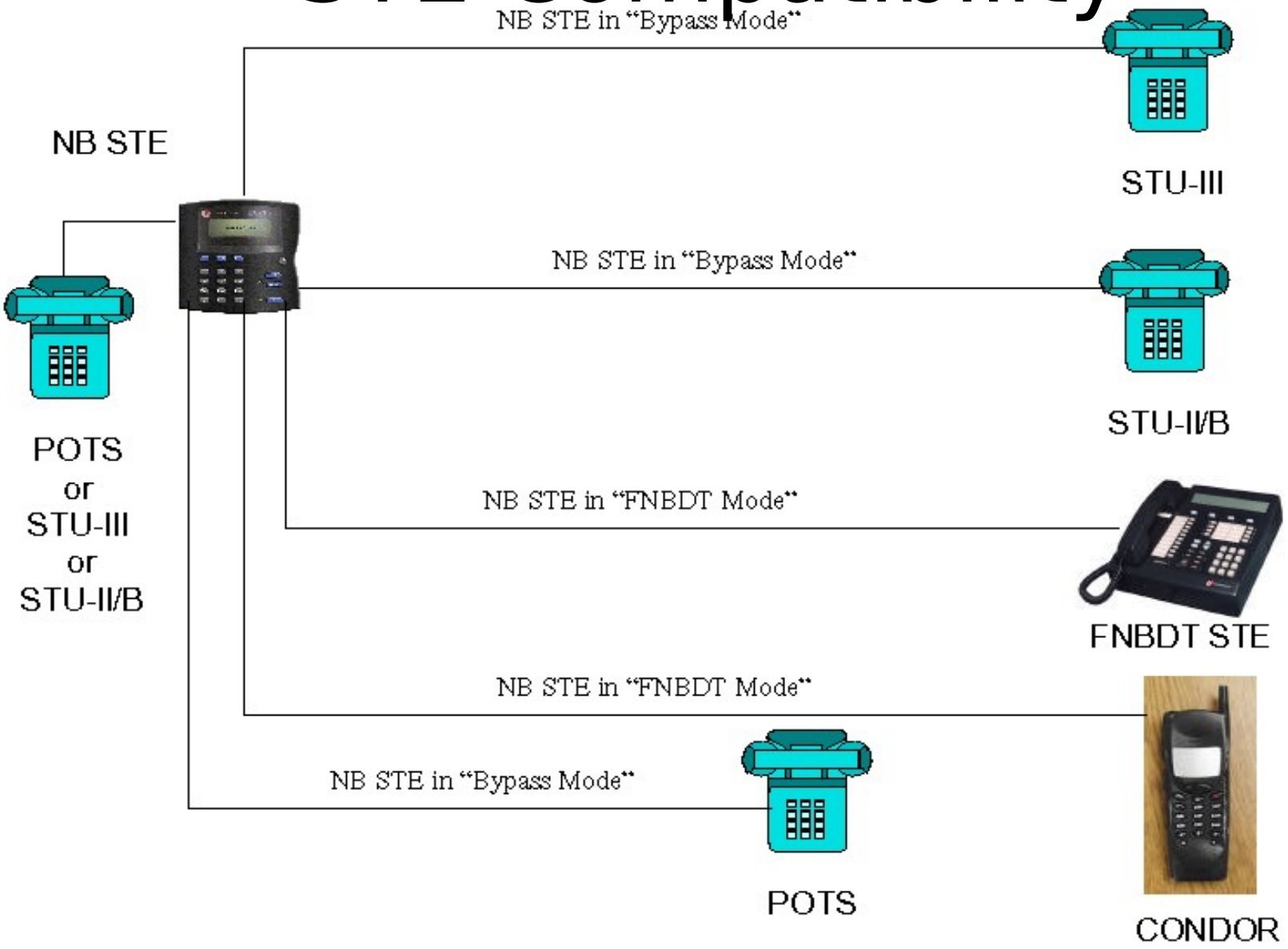
Motorola Satellite Series

- satellite and cellular servic
- type 1 end-to-end security
- Iridium security module attaches to it

STE Interoperability



STE Compatibility



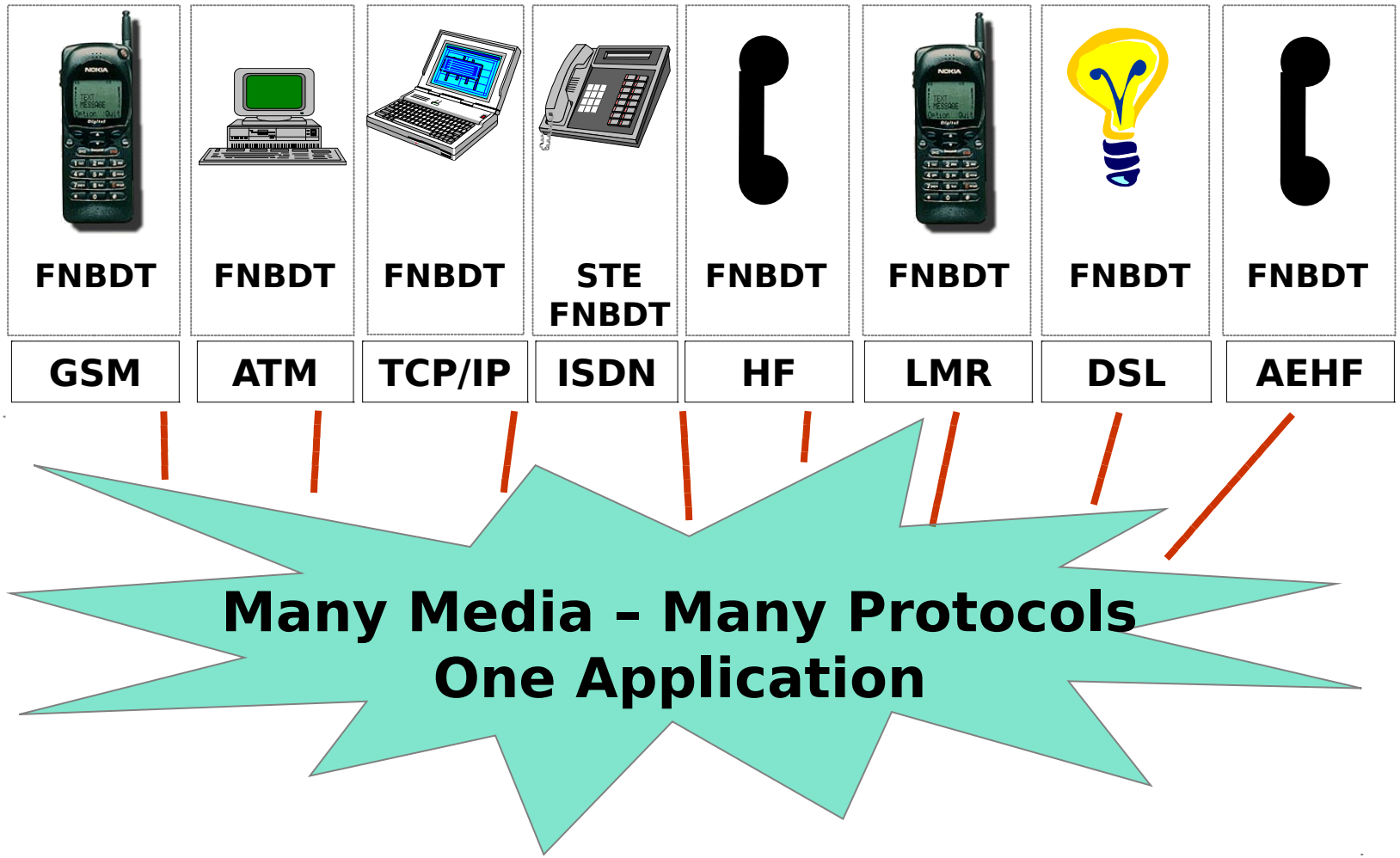
KY-68

- Used with TRI-TAC and MSE
- Operates at 16/32 Kbps with CVSD (wideband)
- Provides encryption of voice or data traffic on switched links to a circuit switch
- No longer being produced

Future Narrow Band Digital Terminal (FNBDT)

- Designed primarily for low-bandwidth, error prone networks such as cell phones
- Secure global interoperability
- FNBDT is an open standard
- Satisfies both NATO and individual nation objectives
- Uses MELP and Forward Error Correction

FNBDT Overview



Military Cryptographic Systems

- Encryption Techniques
- Black/Red Signal
- Cryptographic Standards
- NSA Cryptographic Types
- Layer 1 Military Cryptographic Equipment
- Layer 2 Military Cryptographic Equipment
- Layer 3 Military Cryptographic Equipment
- Telephony Cryptographic Equipment
- Fill Devices
- Key Generators
- Summary

Fill and Storage Devices

- KYK-13
- KOI-18
- KYX-15
- CYZ-10
- KG-83
- KGX-93
- Fortezza Card
- KOV-14
- KSD-64A

KYK-13

- Used to receive, store and load key in electronic form
- Simple fill device that can hold six 128 bit keys
- CCI is unclassified when empty -- takes on highest classification of key resident in memory

KOI-18

- Simple fill device used to read and transform paper key into electronic key
- May be used to directly fill crypto equipment or load another fill device
- Unclassified and has n

KYX-15

- Net control device that can store sixteen 128 bit keys
- CCI that is unclassified when empty - takes on the highest classification of the key in memory
- Used to perform OTAR
- Can be used to generate key locally when used in conjunction with KG-84, KIV-7 or KY-68

AN/CYZ-10

- Data Transfer Device (DTD) can emulate other fill devices
- Receives, audits and transfers 128 bit keys with identification information
- CCI and is unclassified when empty or when the CIK is removed
- Referred to as an ANCD

Simple Key Loader (SKL)

Processor 32-bit Intel® XScale™ CPU (400 MHz)

O/S Win CE.NET (4.1)

RAM 128 MB of SDRAI

ROM 64 MB of Flash M

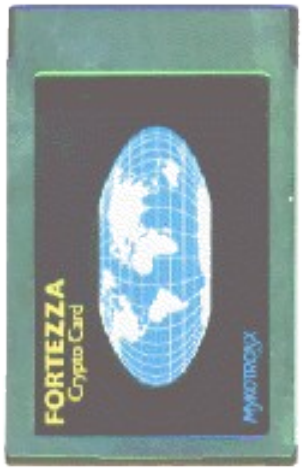
Graphics 2-D Accelerator

Size 7” x 3.5” x 1.8”

Weight Approx 18 oz. 504 gms.

Fortezza Crypto Card (1 of 2)

- Used with DMS to encrypt/decrypt
- 1.5 MBs processing rate
- Tamper proof/ultrasonically welded
- Exportable with State Department approval
- Includes RISC based processor

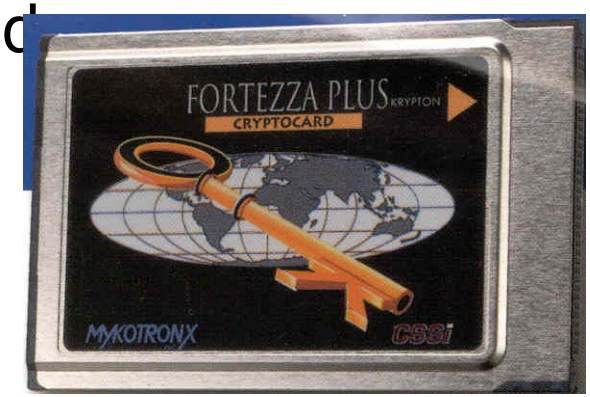


Fortezza Crypto Card (2 of 2)

- Provides Cryptographic Functions
  - Public Key Exchange
  - Message Encryption
  - Digital Signature
  - Hashing
  - Timestamp
  - Password
  - Certificate
- Algorithms used
  - KEA, Skipjack, DSA, SHA-1

KOV-14

- Special PCMCIA card also known as a Fortezza Plus card, which provides all the encryption and other security services
- Used to enable the STE
- Classified to level of keying material
- Unclassified when separated from STE
- Stays with COMSEC Material Control System (CMCS) until destroyed
- With operational key – classified
- With seed key -- unclassified



KSD-64A

- Contains electronic fill information for STU-III
- May contain classified operational key or it may contain unclassified seed key
- Can operate in three modes

KSD-64A Modes

- Operational Key
  - Loaded into a STU-III terminal to make direct secure calls to other STU-IIIs
  - Fill Device
- Seed Key
  - Loaded into a STU-III terminal, enabling it to electronically obtain its operational key during a rekey phone call
  - Fill Device
- Crypto Ignition Key (CIK)
  - Stores an electronic "password."
  - CIK is inserted and turned in the STU-III terminal that shares this "password" to unlock the terminal's secure transmission features
  - Secure mode is locked when the CIK is removed.

KSD-64A

- Once KSD-64A has loaded the key into the STU-III it may be used as a CIK
- CIK and phone together -- highest classification of the keys
- Separated -- CIK and STU III are unclassified
- Stands for Key Storage Device
- Can store 8,000 bytes of info
- Contains Electronically Erasable Programmable Read Only Memory (EEPROM)

STU-III Loading Process

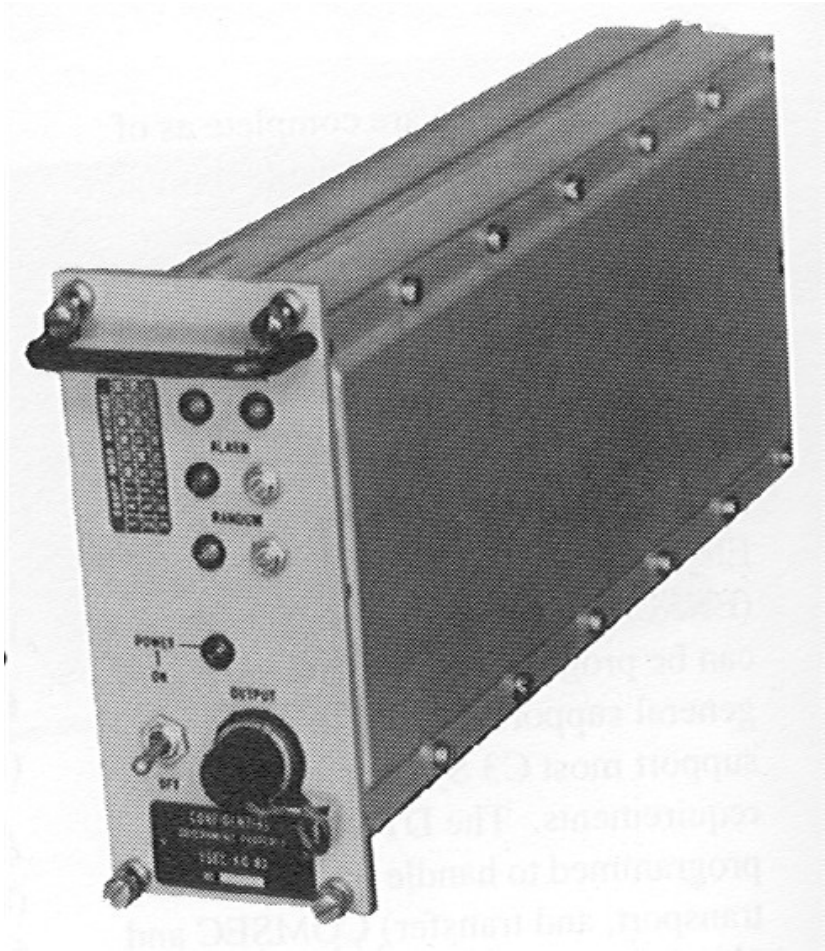
- Order seed key – contains Key Material Identification Number (KMID)
- Load seed key
- Convert seed key to operational key by calling EKMS
  - Also downloads Compromise Information Message/Compromised Key List (CIM/CKL)
  - Operational key is stored in STU-III
  - KSD-64A is now zeroized
- Needed to create CIKs

Key Generators

- KG-83
- KGX-93
- LMD/KP (KOK-22)

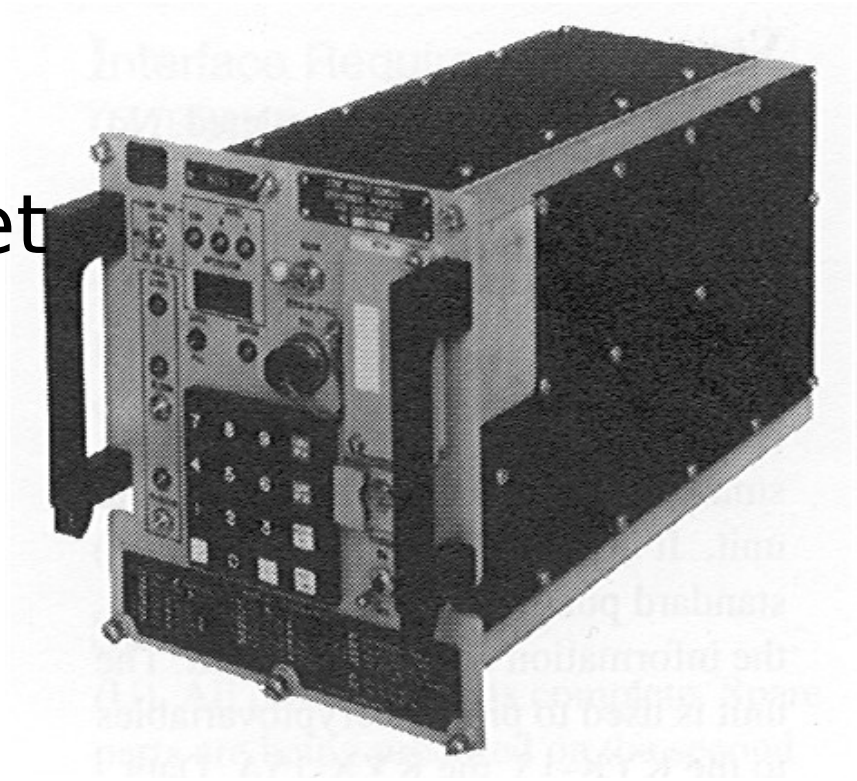
KG-83

- Used in TRI-TAC and stand alone applications
- Generates 128 bit TEK up to Top Secret
- Compatible with most COMSEC equipment that accepts 128 bit key
- Requires initial/annual certification



KGX-93

- Used in MSE and TRI-TAC switches
- Generates 128 bit key up to Top Secret
- Can also store key
- Requires initial/annual certification



Local Management Device/Key Processor (LMD/KP)

- 128 bit key
- Key Processor
  - KOK-22A
  - Key Generation
- Local key generation, distribution, auditing and reconciliation
- Access to ACCOR
- Tier 2 of EKMS
- Can load 1000 keys at once